AMENDMENTS TO THE CLAIMS

1.   (Currently amended) An RFID system comprising:

a plurality of RFID transponders configured to receive a signal and [[and]] to generate a response signal based thereon, said RFID transponders having a random number generator usable to determine whether to respond to a received message addressed to said plurality of RFID transponders;

a host computer configured to generate a message for transmission to at least one of said RFID transponders; and

at least one interrogator communicatively coupled to said host computer having an interrogator transmitter and an interrogator receiver which operate in half-duplex mode, wherein said interrogator transmitter is capable to transmit messages received from said host computer to said plurality of RFID transponders during a first part of said half-duplex mode and provide an illumination signal to said plurality of RFID transponders during a second part of said half-duplex mode, and said interrogator receiver is capable to receive a signal generated by said at least one of said RFID transponders and provide said received signal to said host computer;

wherein said host computer is configured to identify a unique identification code associated with each of said plurality of RFID transponders by iteratively transmitting a message including a variable having a predetermined value to said RFID transponders, and only said RFID transponders which generate a random number greater than said variable respond to said message by transmitting the identification codes associated with said respective RFID transponders.

2.   (Previously presented) The RFID system of Claim 1, wherein said signals are transmitted in spread spectrum format.

IVEN\25541AM2.DOC

3.   (Previously presented) The RFID system of Claim 1, wherein communications between said at least one interrogator and said plurality of RFID transponders is in TDMA format in which a number of time slots are available for transmission.

4.   (Previously presented) The RFID system of Claim 3, wherein said RFID transponders which generate a random number greater than said variable are also configured to use said generated random variable to determine which time slot to use for transmission of said response signal.

5.   (Previously presented) The RFID system of Claim 1, wherein said host computer is configured to intelligently adjust said variable after receipt of a response signal to ensure that an adequate number of responses are received during a next iteration.

6.   (Previously presented) The RFID system of Claim 1, wherein an RFID transponder is further configured to use said random number generator to generate a unique identification code.

7-8.   (Canceled)

9.   (Previously presented) A method for generating identification codes for a plurality of RFID transponders, comprising:

transmitting a re-select identification code command to a plurality of RFID transponders;

generating, at said plurality of RFID transponders, a first random number and calculating a new identification code based upon said random number;

iteratively transmitting a read identification code command and a variable having a predetermined-value from a host to said plurality of RFID transponders;

receiving, at said plurality of RFID transponders, said read identification code command and said variable;

generating, at said plurality of RFID transponders, a random number;

IVEN\25541AM2.DOC

comparing, at said plurality of RFID transponders, said variable with said generated random number;

transmitting, by said RFID transponders where said generated random number is greater than said variable, the new identification code associated with said RFID transponder and then becoming inactive such that said RFID transponder does not respond to further read identification code commands during a current read identification code process;

waiting, by said RFID transponders where said generated random number is not greater than said variable, for a next transmission of said read identification code command and said variable;

intelligently adjusting, by said host, the value of said variable for the next transmission of said read identification code command and said variable; and

examining said variable at said host and ceasing the iterative transmission of said read identification code command when no RFID transponders respond by transmitting their new identification code in response to a final value of said variable.

10.   (Previously presented) The method of Claim 9, wherein said predetermined value for said variable is set as a high value, said intelligently adjusting the value of said variable reduces the value of said variable, and wherein said final value is zero.

11.   (Previously presented) An interrogator for communicating with an RFID transponder in an RFID system, comprising:

at least one antenna;

a transmitter coupled to said at least one antenna and configured to transmit an FSK modulated spread spectrum signal on said at least one antenna during a transmitting mode and a BPSK modulated spread spectrum signal during a receiving mode;

IVEN\25541AM2.DOC

a receiver coupled to said at least one antenna and configured to receive a spread spectrum signal in PSK format; and

a controller coupled to said transmitter and said receiver and configured to control said transmitter and said receiver.

12. (Previously presented) The interrogator of Claim 11, wherein said at least one antenna comprises a first antenna having a first polarization and a second antenna having a second polarization which is orthogonal to said first polarization, and further comprising an antenna switch matrix configured to select one of said first antenna and second antenna for coupling to said transmitter and a second of said first antenna and said second antenna for coupling to said receiver.

13. (Previously presented) The interrogator of Claim 12, wherein said at least one antenna further comprises a third antenna having a third polarization which is orthogonal to said first polarization and to said second polarization, and said antenna switch is configured to select one of said first antenna, second antenna and third antenna for coupling to said transmitter and a second of said first antenna, second antenna and third antenna for coupling to said receiver.

14. (Previously presented) The interrogator of Claim 11, wherein said transmitter comprises:

an FSK transmitter section configured to generate a message for transmission as a spread spectrum output signal in FSK format;

a BPSK transmitter section configured to generate an illumination signal for transmission as a spread spectrum signal in BPSK format;

an output amplifier; and

a switch configured to selectively couple said FSK transmitter section or said BPSK transmitter section to said output amplifier.

IVEN\25541AM2.DOC

15. (Previously presented) The interrogator of Claim 14, wherein said FSK transmitter section comprises:

a Manchester encoder coupled to said controller;

a PN generator coupled to said controller; and

an FSK modulation generator coupled to said Manchester encoder and said PN generator.

16. (Previously presented) The interrogator of Claim 14, wherein said BPSK transmitter section comprises:

a PN generator;

a low noise oscillator; and

a balanced modulator coupled to said PN generator and said low noise oscillator.

17. (Previously presented) The interrogator of Claim 11, wherein said receiver comprises:

a band pass filter having an input coupled to said at least one antenna for receiving a signal;

a first mixer and a second mixer each having a first input coupled in parallel to an output of said band pass filter and a second input coupled to a signal derived from a transmitted signal;

a first bandpass filter coupled to an output of said first mixer;

a first data and clock recovery circuit coupled to an output of said first bandpass filter for recovering an in-phase version of said received signal;

a second bandpass filter coupled to an output of said second mixer; and

a second data and clock recovery circuit connected to an output of said second bandpass filter for recovering a quadrature-phase version of said received signal.

18-19. (Canceled)

IVEN\25541AM2.DOC

20. (Previously presented) A transponder for communicating with an interrogator in an RFID system, comprising:

a first antenna element having a first predetermined dimensional configuration;

a second antenna element having a second predetermined dimensional configuration;

an impedance modulator coupled between said first antenna element and said second antenna element which causes said first antenna element to be electrically coupled to said second antenna element in a first state and to be electrically isolated from said second antenna element in a second state;

a receiver configured to receive a message within an FSK modulated spread spectrum signal, said receiver being coupled to said first antenna element, said second antenna element and said impedance modulator; and

a controller coupled to said receiver, said controller being configured to receive said message and selectively respond to said message in PSK format by reflecting an illumination signal transmitted by said interrogator by selectively switching said impedance modulator between said first state and said second state.

21. (Previously presented) The transponder of Claim 20, wherein said receiver comprises:

a frequency discriminator having an input coupled to said first and second antenna elements;

a bandpass quantizer having an input connected to an output of said frequency discriminator; and

a low pass filter connected to an output of said bandpass quantizer.

IVEN\25541AM2.DOC

22. (Original) The transponder of Claim 20, wherein said first predetermined dimensional configuration is a length of one-quarter wavelength and said second predetermined dimensional configuration is a length of three-quarter wavelength.

23. (Previously presented) The transponder of Claim 22, wherein said first antenna element is comprised of two first sub-elements coupled at a ninety degree angle.

24. (Previously presented) The transponder of Claim 23, wherein said first sub-elements have a predetermined length relationship to each other.

25. (Previously presented) The transponder of Claim 22, wherein said second antenna element is comprised of a plurality of second sub-elements coupled at ninety degree angles in a geometrically folding configuration.

26. (Previously presented) The transponder of Claim 25, wherein said second sub-elements have a predetermined length relationship to each other.

27. (Original) The transponder of Claim 20, wherein said first antenna element and said second antenna element together form a dipole configuration.

28. (Previously presented) A method of generating a random number in an RFID transponder, comprising:

calculating a random seed based upon a difference between a local clock signal and a clock signal derived from either a received signal or random noise;

supplying said random seed to a random number generator; and

generating a random number based upon said random seed.

29. (Previously presented) An apparatus for generating a random number, comprising:

a first clock input derived from a local clock oscillator;

a second clock input derived from a received signal or random noise; and

IVEN\25541AM2.DOC

means coupled to said first clock input and said second clock input for generating a random number based upon a timing difference between said first clock input and said second clock input.

30-32. (Canceled)

33.   (Previously presented) A method for a host having a plurality of transmitting antennas to read an identification code from a plurality of RFID transponders having unique identification codes, comprising:

iteratively transmitting a read identification code command and a variable having a predetermined value from said host to said plurality of RFID transponders on each of said plurality of transmitting antennas;

receiving, at said plurality of RFID transponders, said read identification code command and said variable;

generating, at said plurality of RFID transponders, a random number;

comparing, at said plurality of RFID transponders, said variable with said generated random number;

transmitting, by said RFID transponders where said generated random number is greater than said variable, an identification code associated with said RFID transponder and then becoming inactive such that said RFID transponder does not respond to further read identification code commands during a current read identification code process;

waiting, by said RFID transponders where said generated random number is not greater than said variable, for a next transmission of said read identification code command and said variable;

receiving at said host said transmitted identification codes associated with particular RFID transponders and storing said identification codes and associated antenna information in

memory so that further communication with a particular one of said plurality of transponders is performed by using said identification code and said antenna information;

intelligently adjusting, by said host, the value of said variable for the next transmission of said read identification code command and said variable; and

examining said variable at said host and ceasing the iterative transmission of said read identification code command when no RFID transponders respond by transmitting their identification code in response to a final value of said variable.

34. (Previously presented) An RFID system for tracking election ballots comprising:

a plurality of RFID transponders connected to separate ballots, and configured to receive a signal and to generate a response signal based thereon, said RFID transponders having a memory configured to store election data and a random number generator usable to determine whether to respond to a received message addressed to said plurality of RFID transponders;

a host computer configured to generate a message for transmission to at least one of said RFID transponders and control the storage of election data within the memory of said RFID transponders connected to said ballots; and

at least one interrogator communicatively coupled to said host computer having an interrogator transmitter and an interrogator receiver which operate in half-duplex mode, wherein said interrogator transmitter is capable to transmit messages received from said host computer to said plurality of RFID transponders during a first part of said half-duplex mode and provide an illumination signal to said plurality of RFID transponders during a second part of said half-duplex mode and said interrogator receiver is capable to receive a signal generated by said at least one of said RFID transponders and provide said received signal to said host computer;

wherein said host computer is configured to identify a unique identification code associated with each of said plurality of RFID transponders by iteratively transmitting a message

IVEN\25541AM2.DOC

including a variable having a predetermined value to said RFID transponders, and only said RFID transponders which generate a random number greater than said variable respond to said message by transmitting the identification codes associated with said respective RFID transponders.

35.   (Previously presented) The RFID system of Claim 34, wherein said host computer selectively transmits a predetermined message which causes each RFID transponder receiving said predetermined message to transmit its identification code to said host computer.

36.   (Previously presented) The RFID system of Claim 35, wherein said host computer is configured to continuously transmit said predetermined message and receipt of said identification code by said host signals an alarm event.

37.   (Previously presented) In a communications system having a first device having a transmitter and a receiver and a plurality of second devices having a transmitter and a receiver, where communications between said first device and said plurality of second devices is in TDMA format having a plurality of time slots for transmission, a method for determining if more than one second device has transmitted a signal to said first device at the same time during a current TDMA communications period, comprising:

sampling the relative power in an analog baseband channel of said receiver in said first device during each of said time slots;

sampling the relative power in an analog baseband channel of said receiver in said first device during a period of no communications;

comparing said sampled relative power in each of said time slots to said sampled relative power in said period of no communications;

setting, if said comparison for a particular one of said time slots produces a value of greater than unity by a predetermined amount, said particular time slot to be occupied;

IVEN\25541AM2.DOC

determining which of said time slots did not have an accepted message;

comparing said time slots which did not have an accepted message to said occupied time slots; and

determining that each of said time slots which did not have an accepted message and which is occupied represents a time slot in which more than one second device transmitted a message at the same time.

38.   (Previously presented) The interrogator of Claim 17, wherein said first data and clock recovery circuit comprises a first digital discrete phase lock loop circuit configured to synchronize to first signals input to said first data and clock recovery circuit, said second data and clock recovery circuit comprises a second digital discrete phase lock loop circuit configured to synchronize to second signals input to said second data and clock recovery circuit, and said controller is configured to choose between said in-phase version of said received signal and said quadrature-phase version of said received signal based upon which of said first and second digital discrete phase lock loop circuit first synchronizes to said first and second input signals, respectively.

39-49. (Canceled)

IVEN\25541AM2.DOC